IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant(s): | Mark L. Wilkinson, Ronald J. Miller, Michael J. McDaniels | | |
| Assignee: | Mirage Networks, Inc. | | |
| Title: | Deterring Network Incursion | | |
| Serial No.: | 10/676,637 | Filing Date: | October 1, 2003 |
| Examiner: | Unassigned | Group Art Unit: | 2143 |
| Docket No.: | MIR0003US | | |

Irvine, California
August 22, 2006

Commission for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REVISED PETITION TO MAKE SPECIAL UNDER 37 CFR §1.102(d)

Dear Sir:

In response to the Decision on Petition dated June 22, 2006, the applicants hereby submit this revised petition pursuant to 37 CFR §1.102(d) and MPEP §708.02(VIII) to make the above-identified application special.

The instant application presents claims directed to embodiments of a single invention. Should the Office determine that all the claims presented are not obviously directed to embodiments of a single invention, the applicants will make an election without traverse as a prerequisite to the grant of special status.

The applicants submit that a pre-examination search has been performed by a professional search firm in the following classes/subclasses:

| Class | Subclasses |
|---|---|
| 709 | 223, 224, 225 |
| 713 | 201 |
| 726 | 13, 22, 23 |

Copies of the following references believed to be the most closely related to the subject matter encompassed by the claims were also filed on January 23, 2006:

| Patent/Publication No. | Inventor | Issue/Publication Date |
|---|---|---|
| 5,884,025 | Baehr *et al.* | March 16, 1999 |
| 2004/0044912A1 | Connary *et al.* | March 4, 2004 |
| 6,725,378 | Schuba *et al.* | April 20, 2004 |

A preliminary amendment to claims 1, 3, 5, 6, 11, 16, 42, 44, 47-49, 57, 59, 62-64, 72, 74, and 77-79 was filed on January 23, 2006. The references listed above are evaluated herein in view of the amended claims.

## ***Detailed Discussion of the References***

**U.S. Patent No. 5,884,025 (Baehr et al.)** discloses a system for screening data packets as they arrive on a network for security threats. (See Baehr, Abstract.) Baehr's system intercepts a packet, screens the packet based on various pieces of information, and determines an action to take regarding the packet including dropping, blocking, altering, or allowing the packet. *(Id.;* Baehr, column 2, lines 10-49.)

As the title "System for Packet Filtering of Data Packets at a Computer Network Interface" suggests, Baehr's system is designed to control packets flowing into (and out of) a protected private network. (See Baehr, column 7, lines 5-16 and column 8, lines 27-37.) If a packet is received from an external source address that is regarded as a threat, the packet is prevented from entering the private network. (See *Id.;* see also column 9, lines 60 - 67.) No further examination of the packet is performed before determining a response to the packet, as required by independent claims 1, 42, 57, and 72. Furthemore, Baehr's system is limited to dealing with external threats. Baehr's system does nothing to prevent distribution of infected packets internally after the network has been infected.

Independent claim 1includes "determining whether a source address for a first packet sent by the source address to a destination address qualifies as a threat; examining the first packet; and determining a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat." This combination of features is not taught or suggested by Baehr.

Independent claim 42 includes

> "threat-determining means for determining whether a source address for
> a first packet sent by the source address to a destination address
> qualifies as a threat;
> examining means for examining the first packet; and
> response-determining means for determining a response to the first
> packet based upon the examining and based upon whether the
> source address qualifies as the threat."

In contrast, Baehr does not include "response-determining means for determining a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat."

Independent claim 57 includes

> "a threat-determining module configured to determine whether a source address for a first packet sent by the source address to a destination address qualifies as a threat;
> an examining module configured to examine the first packet; and
> a response-determining module configured to determine a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat."

In contrast, Baehr does not include "a response-determining module configured to determine a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat."

Independent claim 72 includes

> "threat-determining instructions configured to determine whether a source address for a first packet sent by the source address to a destination address qualifies as a threat;
> examining instructions configured to examine the first packet; and
> response-determining instructions configured to determine a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat."

In contrast, Baehr does not include "response-determining instructions configured to determine a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat."

Furthermore, dependent claim 5, *inter alia*, includes "determining whether the source address is on a local network." This feature is not disclosed or suggested by Baehr.

Accordingly, Baehr does not teach the limitations of claims 1, 42, 57, and 72. Therefore, independent claims 1, 42, 57, and 72 and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable for at least these reasons.

Furthermore, independent claims 41, 56, 71, and 86 include replacing the destination address with a hardware address for a device to receive communication targeted to the destination address when the destination address is the synthetic hardware address. Baehr does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a valid hardware address. Consequently, independent claims 41, - 4- 56, 71, and 86 are allowable over Baehr for at least these reasons.

U.S. Patent No. 6.725.378 (Schuba et al.) discloses a system and method for protecting networks from intrusions, specifically denial of service attacks. The system includes a means for monitoring incoming data on a network, determining if a packet is suspect, and categorizing the packet source address as unacceptable, suspect, or acceptable (See Schuba, column 2, lines 1-5, and Fig. 4). If a packet is found to have an unacceptable source address, the packet is placed in an "unacceptable address state." *(Jd.)* As described therein, the unacceptable address state "do[ es] not involve any appreciable amount of processing beyond the states shown in Fig. 4." (See Schuba, column 9, lines 16-20 and 33-37.) Fig. 4 step 72 indicates that a reset message is sent to close the spurious connection to the unacceptable source address. (See Schuba, column 9, lines 23-32.) No further processing of the packet is performed. (See Schuba, column 9, lines 16-20 and 33-37.)

In contrast, the independent claims 1, 42, 57, and 72 determining "a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat." Even if the source address is classified as a threat initially, the packet is nevertheless examined and a response to the packet is determined based upon the examination and whether the source address is a threat. Consequently, independent claims 1, 42, 57, and 72 and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable over Schuba for at least these reasons.

Furthermore, independent claims 41, 56, 71, and 86 include replacing the destination address with a hardware address for a device to receive communication targeted to the destination address when the destination address is the synthetic hardware address. Schuba does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a hardware address. Consequently, independent claims 41, 56, 71, and 86 are allowable over Schuba for at least these reasons.

U.S. Patent Application 2004/0044912 (Connary et al.) discloses a method for determining a network security threat. Network devices are monitored to aggregate all event data generated by monitored devices to provide a network ranking of al1 network activity. (See Connary, Abstract.) A threat level for a given host is determined by a threat weighting assigned to that host and a threat weighting assigned to that host's netblock. *(Id.)*

In one embodiment, a sensor detects network events and records data regarding such events. (See Connary, paragraph [0008].) The event data can include, for example, information about the sensor detecting the event, source and destination IP addresses associated with the event, source and destination ports, and/or the type of event (e.g., "Get request," accept, reject, etc.). *(Id.)* Event data also includes a time and date of receipt that a management module received the event data. (Connary, paragraph [0009].)

Applicants respectful1y submit that the analysis performed by Connary's system requires examination of more than one packet. Connary's system accumulates event data and processes the event data by multiple modules before the nature of the threat posed by the event data can be determined. (See Connary, paragraphs [0008] through [0010].) In contrast, independent claims 1, 42, 57, and 72 determining "a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat." Connary does not disclose or suggest these features. Accordingly, independent claims 1,42, 57, and 72, and respective dependent claims 2-40, 43-55, 58-70, and 73-85 are allowable over Connary for at least this reason.

Furthermore, independent claims 41, 56, 71, and 86 include replacing the destination address with a hardware address for a device to receive communication targeted to the destination address when the destination address is the synthetic hardware address. Connary does not teach the concept of a synthetic hardware address or of replacing a synthetic hardware address with a hardware address. Consequently, independent claims 41, 56, 71, and 86 are allowable over Connary for at least these reasons.

## ***Conclusion***

In summary, Applicants respectfully submit that none of the references located during the pre-examination search, or otherwise made of record by Applicants, teaches or suggests (at least) examining a packet and determining a response to the packet based upon the examination and whether the source address qualifies as a threat. Accordingly, Applicants respectfully submit that claims 1-86 are allowable over all of the above references.

Applicants respectfully request that this petition be granted, and that the present application receive expedited examination. Should any issues remain that might be subject to resolution through a telephone interview, the Office is requested to contact the undersigned at 949.350.7301.

I hereby certify that this correspondence is being transmitted to the USPTO on the date shown below:

/Mary Jo Bertani/
(Signature)

Mary Jo Bertani
(Printed Name of Person Signing Certificate)

August 22, 2006
(Date)

Respectfully submitted,

/Mary Jo Bertani/

Mary Jo Bertani
Attorney for Applicant(s)
Reg. No. 42,321